Information Assurance Security Awareness Brief

Marine Forces Pacific

Information Assurance Defined

- **Information operations that protect and defend information and information systems be ensuring their availability, integrity, authentication, confidentiality and non-repudiation… providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.” CNSSI 4009**

Information Classification

- **All information processed at MARFORPAC is considered to be, at the lowest classification, SENSITIVE and must be treated as such.**
- **Guiding Reference OMB Circular A-130**

Login Banner

- **Read it!**
- **By clicking OK you acknowledge that:**
  - the information system you are using is for "Official Government Use Only"
  - your computer and all information it contains are subject to inspection
  - your actions are subject to continuous auditing

Password Protection

- **Personal passwords must remain private**
  - Don’t write it down
  - Don’t type a password while others watch
  - Don’t tell it to anyone over the phone, even a system administrator
  - Don’t record password on-line or e-mail it
  - Don’t use easily guessed words
    - SemperFi! ,Marines, DevilDog1
  - 8 characters, alpha-numeric, special characters
    - h0M3rUn#
- **Ref: MARADMIN 089/03**

Remember

- **Protect your username and password**
- **Use strong passwords**
- **Lock your computer when you step away**
- **Use your CAC to sign and encrypt sensitive email**

Appropriate Use of the Internet

- **Official Use**
- **Support USMC Mission**
- **Improve Professional Skills or Formal Academic Education**
- **Does not Adversely Affect Professional Duties**
- **Improving Morale**
- **Does NOT Adversely Reflect Upon The Corps**
- **Downloading any obscene or hate content is prohibited.**
- **Every connection to the Internet is logged and reviewed.**

Appropriate Use of E-Mail

- **Accessing commercial/web-based E-Mail services from MCEN not authorized**
  - Hotmail.com, AOL.com, Yahoo.com, etc…
- **Can RECEIVE or SEND personal messages from MCEN to commercial accounts**
- **"UNDER NO CIRCUMSTANCES WILL OFFICIAL GOVERNMENT CORRESPONDENCE OR DATA FILES BE SENT OR FORWARDED TO, OR CREATED OR STORED ON, COMMERCIAL E-MAIL SERVICES. THIS INCLUDES, BUT IS NOT LIMITED TO, FORMAL MESSAGE TRAFFIC, WORKING DOCUMENTS AND PERSONAL OFFICIAL E-MAIL."**

Prohibited E-Mail Usage

- Illegal Activities
- Partisan Activity or Lobbying on Behalf of Organizations NOT Affiliated With the Corps or DoD
- Accessing, Storing, Displaying or Distributing Obscene Materials
- The Creation, Forwarding or Passing of Chain Mail

Audit (Monitoring)

- **All activity on the MARFORPAC Network is monitored to:**
  - Ensure system performance
  - Determine probable causes and impacts
  - All logs subject to review by authorized personnel.
  - E-Mail, Web Surfing, etc. is ALL recorded.
  - **Read your logon warning banner**.

Anti-Virus Software

- **Computer viruses are a real threat to the MARFORPAC Network**
- **Anti-Virus software is available for HOME USE for all DOD personnel: http://www.cert.mil/antivirus/av_info.htm**
- **Anti-spyware software is also available for home use for DoD personnel: https://iase.disa.mil/sdep/**
- **All media must be scanned for possible viruses when transferring files**

How Computer Viruses Spread

- Email attachments (by opening them; if it is an executable file)
- Downloading files from the Internet
- Sharing software
- Commercial software
- Shareware/Freeware
- Third-party use of your computer

Viruses: What To Look For

- **Note abnormal or unexpected activity**
  - Displays, music, or other sounds
  - Slowdown in processing speed
  - Disk activity
  - Error messages
  - Changes in file sizes
  - Loss of programs or data

If You Suspect an Infection

- **STOP processing**
- **Disconnect Network Cable from PC**
- **Scan all local, physical drives on your PC.**
- **Contact the Information Assurance Office**
- **Information Assurance Office: 477-8884/8492**
- **If infected, wait for further instructions**
- **New viruses appear daily**

Peer-to-Peer (P2P) File Sharing

- **P2P poses a serious threat to the security and integrity of our networks**
- **P2P software is strictly prohibited on all Government information systems**
- **Currently over 100 different P2P programs released (Grokster, LimeWire, Gnutella, BitTorrent, etc…)**
- **Malicious Code (Viruses, Spyware, Backdoors & other Malware)**
  - P2P programs often create a backdoor or back channel that can be manipulated by someone else.

Why P2P is a Serious Threat

- **Sensitive information leakage**
- **Child pornography (P2P programs are often used to trade child porn)**
- **Many of the P2P exchanged files are illegal copies of music, video, or software programs which have been legally copyrighted or licensed by their owners.**
- **Transfer or ownership of these pirated files may result in legal or disciplinary action should the transferred file be acquired unlawfully.**
- **Opens up the Command to legal ramifications if pirated files are found on government-owned systems.**

Wireless Security

- **One unsecure Wireless Access Point (WAP) can**
  - Allow unrestricted access to your network
  - Opens a hole into the MCEN
- **MC Op Standard 014 – Wireless Local Area Networks**
- **All wireless devices MUST be approved by HQMC C4 and the MCEN DAA**
  - Layer 2 security required for UNCLAS
  - SECNET-11 Only approved product for SECRET

Incident Reporting

- **Report any unusual or suspicious activity to local Information Assurance Office (477-8884/8492)**
  - Attempting unauthorized access
  - Abuse of authorized privileges
  - Use of privately-owned or unapproved software
  - Violation of copyright laws
  - Deliberate introduction of viruses
  - Forwarding or Creation of chain mail
  - Unauthorized disclosure of classified material

User Responsibilities

- **Protect sensitive information**
- **Use government AIS & software for authorized use only**
- **Report suspected compromises**
- **<u>DO NOT</u> try to bypass security settings**

Local Command Rules of Behavior

- **MARINE FORCES PACIFIC HEADQUARTERS**
- **LOCAL AREA NETWORK**
- **ACKNOWLEDGEMENT OF RESPONSIBLITIES**
- **REF: (a) MARFORPAC 5239 – Information System Security Plan**
- **(b) MARFORPACO 5510.17A – SOP for Secure Operation of Automated Information Systems**
- **(c) COMPUTER SECURITY ACT of 1987**
- **(d) MARADMIN 162/00 – Appropriate use of Government Information Technology Resources**
- **_____Every user of the MARFORPAC LAN is responsible for protection of the data which the system stores, processes or transmits. In concert with the references this checklist provides a basic guideline in order for the user to acknowledge their preliminary responsibilities and maintain a proper level of Information System Security (INFOSEC). Failure to comply with these provisions may result in the removal of your LAN Privileges, PC, or prosecution in the event of criminal activity.**
- **_____All personnel are required to attend an information system security (INFOSEC) class. Additionally, users requiring a Secure Account will possess a SECRET Clearance. If you haven't attended one in the past 11 months, request a class via your section Information System Coordinator (ISC) or the network security section (477-8305).**
- **_____All AIS equipment, media (disks), and hard copy printouts from LAN printers will be properly labeled with the level of classification of data processed. Classified floppy disks, removable hard drives and paper printouts must handled and stored in the exact same way as all other classified material.**
- **_____Contractor/privately owned PCs shall NOT process classified data under ANY circumstances.**
- **_____All software executing on PC's shall be properly licensed. All MARFORPAC personnel are accountable to the Designating Approving Authority (DAA) to ensure all software executing on PC's has been approved by the G6. If privately owned or unauthorized software (e.g., game software) is discovered, the software will be removed and a report submitted to the offender's supervisor and ISSM.**
- **_____Passwords are the first line of defense every individual can control in terms of INFOSEC. DO NOT use easily guessed passwords. Don't tape passwords to desks, walls, or terminals. Use combinations of letters and numbers, both upper and lower. Do not share passwords with anyone. If you do, even with a help-desk individual while troubleshooting a problem with your PC, immediately change it.**

Local Command Rules of Behavior

- **____A computer virus is a program that infects other data files or programs by modifying, destroying, or preventing access to them. Like a real (medical) virus, computer viruses can spread quickly across the LAN and render it useless in a short period of time. Norton AntiVirus is the MARFORPAC standard and is installed on all AISs. Ensure that you scan your system and all floppies routinely and promptly report any discovered viruses to the network help desk (477-8520) or network security section.**
- **____Never leave your AIS system unattended, at a minimum use a time activated screen saver with password protection. Always log off the LAN, turn off your PC (excluding GCCS Workstations) and printer when you depart for the day.**
- **____If transferring data files from an UNCLASS machine to a CLASSIFIED machine (NIPRNET to SIPRNET) the following procedure must be followed. Insert a floppy diskette into the UNCLASS computer and scan the disk for viruses. If no viruses are found, copy the needed files to the diskette. Remove the diskette from the UNCLASSIFIED computer and write-protect it using the write-protect tab. Re-insert the diskette into the drive and copy the needed UNCLASS files to the CLASSIFIED machine. NOTE: IF THIS PROCESS IS NOT FOLLOWED AND THE DISKETTE IS NOT WRITE-PROTECTED PRIOR TO COPYING THE FILES TO THE CLASSIFIED COMPUTER, THE DISKETTE BECOMES CLASSIFIED AS SECRET.**
- **____In accordance with ref (c), you are being made aware that use of government-owned AIS resources is strictly for official government business. During the initial log-on procedure, a DOD warning banner explains that all information being processed on government AISs is subject to monitoring at all times. This is to ensure proper functioning of equipment and systems, including security, to prevent unauthorized use, violation of statues, and to deter criminal activity. If monitoring reveals possible evidence of AIS security violations, this evidence including identification information about the user, may be provided to the Commander and/or law enforcement officials.**
- **11. ____Government Information Technology Resources are for official use and authorized purposes only. Use of these resources, to include access to the internet, is authorized when work related and determined to be in the best interests of the Federal Government and the Marine Corps. Use should be appropriate in frequency, duration, and related to assigned tasks. Use of Government Information Technology Resources for purposes other than those described is <u>PROHIBITED</u>. Examples of prohibited use include, but are not limited to, the following: Illegal, Fraudulent, or Malicious activities. Unauthorized fundraising. Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography or hate literature. Accessing, displaying, or distributing Web Based Email i.e. Hotmail or Yahoo.**
- **I understand and will comply with the above stated LAN Security requirements. Failure to comply may result in revocation of my account privileges and possible disciplinary actions.**
- **SIGN _____ PRINT NAME _____ DATE _____**

For More Information

- ISC's are the first points of contact for computer problems
- Information Assurance Office

  477-8884

  477-8492

  477-8304
- NMCI Helpdesk

  1-866-843-6624

References

- DoDD 8100.2
- CJCSM 6510.01
- MARADMIN 541/05
- MARADMIN 162/00, INFORMATION ASSURANCE BULLETIN 2-00
- MARADMIN 089/03
- ASD/NII Memo 13 Apr 2004, Elimination of Unauthorized Peer-to-Peer (P2P) File-sharing Applications Across DoD

References

- CJCSM 6510.01
- SUBJ/USE OF COMMERCIAL ELECTRONIC MAIL SERVICES// 1221645Z DEC 04
- SUBJ/EFFECTIVE USE OF DEPT OF NAVY INFORMATION TECHNOLOGY RESOURCES//161108Z JUL 05.
- SUBJ/MANDATORY DNS BLACK HOLE LIST// 111241Z OCT 05
- DISA IA Awareness Training CBT